UNITED STATES DISTRICT COURT

for the

Western District of Arkansas

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
Information Associated with Dropbox, Inc. accounts of Anthony Sanchez or email address asanch2011@gmail.com

Case No. 18cm 70

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that there is now concealed on the following person or property located in the Western District of Arkansas *(identify the person or describe property to be searched and give its location):* See "Attachment A"
This court has authority to issue this warrant under 18 U.S.C. §§ 2703(c)(1)(A) and 2711 (3)(A) and Federal Rule of Criminal Procedure 41

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*: See "Attachment B"

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of 18 U.S.C. § 1030/1832, and the application is based on these facts: Compuer Fraud and Abuse and Theft of Trade Secret Information---See "Attachment C"

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of ___ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Christopher Shudy, SA FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 8/2/18

Judge's signature

City and state: Fayetteville, Arkansas

Erin L. Wiedemann, US Magistrate Judge
Printed name and title

ATTACHMENT A

Property to Be Searched

This warrant applies to any and all information associated with any and all accounts of Anthony Sanchez, and/or email address **asanch2011@gmail.com utilized from October 1, 2015 until April 4, 2016** that is stored at premises owned, maintained, controlled, or operated by **Dropbox, Inc. a company headquartered at 333 Brannan Street, San Francisco, California, 94107**.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Dropbox (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, in the form of emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A for the time period set out in Attachment A:

a. The contents of all files associated with the account;

b. The contents of the shared folder titled "Internal Projects."

c. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

d. The types of service utilized;

e. All records or other information stored at any time by an individual using the account, in the form documents, spreadsheets, emails, pictures, videos, or calendar appointments;

f. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken;

g. All location history data, search history and search queries issued;

h. All known User Agent Strings utilized by the account holders;

i. A list of user accounts linked to the account by SMS, recovery email, secondary email, cookie, or Android device.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of 18 U.S.C. § 1030(a)(2), 18 U.S.C. § 1030(b), and 18 U.S.C. § 1343, those violations involving Anthony Sanchez for each account or identifier listed on Attachment A, information pertaining to the following matters:

- Preparatory steps taken in furtherance of the unauthorized network activity, communications regarding execution of the unauthorized network activity, and information regarding tools used for in furtherance of the unauthorized network activity.
- Records relating to who created, used, or communicated with the account or identifier, including records about their identities and whereabouts

CERTIFICATE OF AUTHENTICITY OF DOMESTIC BUSINESS RECORDS PURSUANT TO FEDERAL RULE OF EVIDENCE 902(11)

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Google Inc., and my official title is _____. I am a custodian of records for Google Inc. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Google Inc., and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;

b. such records were kept in the ordinary course of a regularly conducted business activity of Google Inc.; and

c. such records were made by Google Inc. as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

_____ _____

Date Signature

ATTACHMENT C

UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF ARKANSAS

STATE OF ARKANSAS :
:
: **ss. AFFIDAVIT**
:
COUNTY OF WASHINGTON

Affidavit in Support of Application for Search Warrant

1. I, Christopher M. Shudy, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

2. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been so employed since 2018. I presently am assigned to work at the Little Rock Field Office as a member of the Cyber Squad. Among other things, I am responsible for conducting investigations into a variety of criminal and national security matters, including the investigation of unauthorized computer intrusions.

3. Prior to becoming a Special Agent with the FBI, I was an Intelligence Officer in the United States Air Force. From the years of 2014-2016, I worked in cyber intelligence with a focus on computer intrusions in addition to receiving training on digital forensics.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

I make this affidavit in support of an application for a search warrant. This warrant applies to any and all information associated with any and all Dropbox accounts of **Anthony Sanchez**, and/or email address **asanch2011@gmail.com** that is stored at premises owned, maintained, controlled, or operated by **Dropbox, Inc. (hereinafter Dropbox) a company headquartered at 333 Brannan Street, San Francisco, California, 94107**.

5. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Dropbox to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B.

6. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts I believe necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of the violations of Title 18, United States Code (U.S.C.) § 1030 (Computer Fraud and Abuse Act), are presently located within the above identified Dropbox account. Where statements of others are set forth in this affidavit, they are set forth in substance and in part.

Statutory Authority

7. This investigation concerns alleged violation of Title 18, United States Code, Section 1030 (Computer Fraud and Abuse Act) and 1832 – (Theft of Trade Secrets)

a. Under 18 U.S.C. Section 1030(a)(4), it is a federal crime to knowingly and with the intent to defraud access a protected computer without authorization or exceeding authorized access, and by means of such furthers the intended fraud and obtains anything of value.

b. Under 18 U.S.C. Section 1832, it is a federal crime for whoever with intent to convert a trade secret, that is related to or included in a product that is produced for or placed in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will injure any owner of that trade secret knowingly steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information or without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information A trade secret means any and all forms and types of financial, business, economic information, which the owner takes reasonable measures to keep such information a secret, and the information devices independent economic value, actual or potential, from not being generally known to others who can derive economic value from such. See 18 USC Section 1839(3).

PROBABLE CAUSE

1. In September 2016, Walmart filed a complaint with the FBI which stated that Anthony Sanchez, an employee of Compucom, had illegally accessed Walmart employee's computers and email accounts without authorization to obtain pertinent information related to bid contracts with Walmart. At the time, Compucom held a contract with Walmart to provide computer technical support to its employees. The Walmart complaint further provided that Sanchez repeatedly monitored Walmart employee's emails via a virtual private network (VPN) connection into the Walmart network. Moreover the complainant relayed Sanchez would provide

competitor bids and other business information to Compucom management who in turn used the information. On at least one occasion an altered bid resulted in Compucom obtaining a bid contract.

2. Based on this information, an investigation was opened on September 21, 2016 to determine if there was unauthorized access conducted by employees at Compucom into the Walmart computer (email) system. During the investigation, it was determined that Anthony Sanchez worked at Walmart as a contractor for Compucom between 2014 and 2016. From May to September 2015 he was assigned to build and repair computers. From September 2015 to October 2015, he worked on the Windows 7 Migration team managed by Compucom employee Crystal Brasiola. He transitioned to Level Two (L2) Support in October 2015 where he worked on resolving computer help tickets for Walmart employees. This team was managed by Compucom employee Tom Pitts. Tom Pitts was managed by Compucom employee Asif "Sid" Hussain. Asif Hussain (and the vast majority of employees for Compucom in Bentonville, Arkansas) were managed by Compucom employee Jason Gay. Other key Compucom employees include Mitch Lloyd, Tim Parker, Steve Carter, and Tom Alvey. The range of employees is from Anthony Sanchez as a basic help desk employee up to Tom Alvey a Senior Vice President of Retail at the Corporate Headquarters.

3. As part of his employment, Sanchez had the ability to access Walmart employee email accounts and remotely connect to computer systems if authorized by a help desk ticket passed to his team (L2 support) from the Level One (L1) support team. At one point during his employment, Sanchez was trained to support the Exchange team. The Exchange team was responsible for Walmart's enterprise email system. Sanchez was trained in how to use Exchange from a manual.

4. Some key technologies in the Walmart environment in late 2015 and early 2016 include: Webex, which is a virtual or online meeting method. IM which is an Instant Messenger program similar to other chat applications. Email is virtual mail. VOIP (voice over IP) is a basic telephone technology in many environments.

How Walmart initially learned of information theft:

5. On 3/22/2016, Marina Hoofard, a former Walmart employee, was communicating with Anthony Sanchez via IM. During this chat session, Hoofard and Sanchez were discussing a disciplinary meeting between Hoofard's boyfriend and a supervisor at Walmart named Laura Hartman. During this chat, Sanchez took a photo of an email he obtained from the supervisor's email inbox and sent it to Hoofard. Hoofard then sent the photo to her boyfriend, but also accidentally sent the photo to another friend. This friend is the daughter of another Walmart employee who reported the internal email information to Walmart Security. Walmart then conducted an investigation and found that Sanchez was accessing the email inboxes of multiple Walmart employees ranging from executive management to his colleagues and supervisors.

Key Walmart Employee Interviews

6. On April 25, 2018, a Walmart Support Manager was interviewed by the FBI. Said employee, in addition to being a support manager, also worked with L2 Home Office (HO) support which consisted entirely of Compucom contractors and they were located off-campus at 8th Street and the Otis Corley Building. L2 HO consisted of multiple teams that handle issues with Outlook, Windows, clients, software, and infrastructure that was part of the HO domain on the network. If someone in the HO domain (located in Bentonville or other areas of the country) had an issue with their computer, they called L1 support. L1 support would open a ticket documenting the problem

and what L1 attempted to do to resolve the technical issue. If L1 could not fix the issue, the ticket would be forwarded to L2 support for resolution. L2 had the privileges to access employees email inboxes but only had the authority to do so when a ticket was created. Per the Support Manager the only way one employee can read another employee's email was to have an "Officer Delegation" in which one employee agrees to let someone else access their email.

7. On May 3, 2018, the FBI interviewed a Senior Manager of the client team. The Senior Manager had daily interaction with Compucom and met with Asif Hussain about L2 support. A lot of focus of the meetings with Hussain was on the age of service tickets and things Compucom was working on in the technical environment.

8. The Senior Manager stated that the correct procedure for a technician to access a user's computer was after receiving a service ticket from an end-user, an email should be sent to that end-user by the technician requesting permission to access their computer. The service ticket should be attached in the email sent to the user. This should happen before a technician accessed a user's email.

9. The Senior Manager maintained that he never gave Hussain or anyone permission to get on his computer. Walmart has its own Officer Support Team that handles technical support for the Walmart executive team (Vice Presidents and above).

10. On May 3, 2018, the FBI interviewed the former Senior Director of Infrastructure Services, who held that position during the 2016 timeframe. Compucom lost the "Elevate" business contract possibly in early 2015. Compucom was losing a lot of business at that time. Bids for a new technical project would come in one at a time and the Walmart vendor management office would manage the scope, requirements, and requests for proposal from vendors. Per the Senior Director having access to what other competitors were sending in for their requests for

proposal would give Compucom a competitive advantage.

11. On May 3, 2018, the FBI interviewed the Senior Director for Field Services Technology which provides all software and hardware support to all Walmart stores globally.

12. L1 support personnel would not have the access rights to access other individual's email boxes. L2 support personnel had greater access and skill than L1 support. L2 had access rights that could be used to access email boxes given an authorized purpose or helpdesk ticket. L2 were contractors and were handled by Compucom in late 2015 and early 2016.

13. The Senior Director first became aware of issues with Compucom getting into Walmart personnel mailboxes without authorization when Laurie Hartman came to him regarding an internal email that she was involved in being sent outside Walmart to the child of a co-worker and friend of Hartman. The Senior Director contacted Walmart Information Systems Division (ISD) Information Technology (IT) Security because he was concerned the network may have been breached. ISD IT Security connected with Walmart Global Security and the Walmart Command Center. At some point after these events, Steve Carter (Compucom employee) and Jason Gay (Compucom employee) met with the Senior Director. They said they had a bad employee and that they made changes to fix the issue.

14. Compucom would occasionally reach out after this to see if the incident was going to impact business relationships with Walmart. Later the Senior Director found out that executives at Compucom were aware of what was going on.

15. The FBI provided an email to the Senior Director from Compucom employee Anthony Sanchez to Compucom manager Jason Gay. The email contained Verizon RFP (Request for Proposal) budgetary pricing information sent to Gay on February 29, 2016 in which Jason Gay responds "Thank you... you don't happen to have IBM's yet do you". The Senior Director stated

that this is trade secret information and is key to protect this from competitors. Bidding information is confidential and is not shared among competing bidders. The Senior Director also stated that inside information allows for an advantage to keep business and scope competitors by making adjustments based on the information collected by Compucom.

16. L2 support personnel with Compucom had the level of access they had because they had to be able to deal with problems that could include Exchange servers. A ticket would exist before this activity would be authorized. A request would be handled by ISD IT Security. In no way would Compucom contractors be tasked with conducting internal investigations into Walmart employee email messages. If Compucom came across information that was bid related in their authorized course of technical support, they should not use it in anyway and should recuse themselves from that particular contract or bid.

17. On April 6, 2016, the Senior Director sent an email to other WM Employees entitled "CC Meeting Recap" that he had with Compucom managers Steve Carter and Jason Gay. It stated that approximately "six months ago Jason Gay became aware that the Compucom PC Help Desk manager (Asif Hussain) had knowledge of Walmart data through unauthorized access to email. Asif Hussain approached Jason and said that Walmart had been sending Compucom intellectual property to IBM. When Jason asked how Asif Hussain knew that Walmart had been passing data to IBM, it came to light that he or someone from his team had accessed email without authorization. No investigation was conducted and Walmart was not notified of the incident. Asif was not terminated for this incident. Some months later, Asif was terminated from CC for other reasons."

Master Services Agreement

18. The Master Services Agreement between Compucom and Walmart states, in part:

"persons with authorized access to Wal-Mart information must have a documented genuine business need-to-know prior to access." Further, it states that Compucom "shall exercise necessary and appropriate supervision over its relevant employees to maintain appropriate confidentiality and security of Wal-Mart information."

Interviews of key current or former Compucom employees:

19. During the course of the investigation, Anthony Sanchez was interviewed and stated he had master access to the Walmart computer systems. He would connect to the email inboxes of many Walmart employees, including executives, out of curiosity. When Sanchez told Asif Hussain about his activities, he was told to look for information on Compucom's contract margins and bidding information regarding an upcoming project. Eventually, Sanchez and Hussain would have private meetings in which Hussain would instruct Sanchez on what information he should look for. Sanchez was told by Hussain to monitor contract bidding information to determine what other companies were bidding and what amounts they were bidding on Walmart contracts.

20. Sanchez stated that he would use email and instant messaging to pass stolen information to Hussain. At times, he would type the emails to appear as if they had been forwarded to Sanchez from someone named "Raj" but no such person actually existed. Sanchez felt Hussain was taking credit for the information he was obtaining and eventually began passing it directly to Hussain's supervisor, Jason Gay.

21. During the investigation, Asif Hussain was interviewed and stated that Sanchez entered Walmart employee email accounts and provided information to Compucom management that was used to formulate bids for contracts with Walmart. He stated that Sanchez would provide information to Jason Gay and Tim Parker and that Steve Carter, Mitch Lloyd, Tom Alvey, and Lynda Fang all knew of Sanchez's activity.

22. On both 1/13/2016 and 1/14/2016, in a chat session between anthony.sanchez@compucom.com and jason.gay@compucom.com, Sanchez said he "will share the pictures with you & sid on dropbox" and "heading out to do some more ground work at home."

23. On 1/23/2016, Sanchez invited Hussain to the Dropbox shared folder called "Internal Projects" from the account associated with the email account asanch2011@gmail.com. The invite was sent to Hussain's Compucom email account (asif.hussain@compucom.com) with a message stating "2fa updates can be found in this folder."

24. On 1/25/2016, Sanchez shared a file with Hussain on Dropbox using the "Internal Projects" shared folder from the account associated with the email account asanch2011@gmail.com. The invite was sent to Hussain's Compucom email account (asif.hussain@compucom.com) with a message stating "please find Directors presentation attached."

25. On 5/31/2018 - during an interview, Asif Hussain was shown a recovered chat between Sanchez and Gay talking various items - in which Sanchez states "Will share the pictures with you and sid on Dropbox if he is there can you please let him know?". Hussain stated that Dropbox could have been used due to the size of the files shared. The chat between Sanchez and Gay happened on 1/13/2016.

BACKGROUND CONCERNING ONLINE STORAGE

26. In general, providers like Dropbox ask each of their subscribers to provide certain personal identifying information when registering for an ACCOUNT. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, e-mail addresses, and, for paying subscribers, a means and source of payment (including any credit or bank account number). Providers typically retain certain transactional information about the

creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account, and other log files that reflect usage of the account. In addition, providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the ACCOUNT.

27. In some cases, ACCOUNT users will communicate directly with a provider about issues relating to their account, such as technical problems, billing inquiries, or complaints from other users. Providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

CONCLUSION

28. Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on Dropbox who will then compile the requested records at a time convenient to it, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

REQUEST FOR SEALING

29. I further request that the Court order that all papers in support of this application, including the affidavit, search warrant, and search warrant return be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor

known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Respectfully submitted,

Christopher M. Shudy
Special Agent
Federal Bureau of Investigation

Affidavit subscribed and sworn to before me this 2 day of August 2018

Erin L. Weidermann
United States Magistrate Judge